3 Reg.

Interagency Group/Countermeasures
Washington, D.C. 20505

Meet

D/ICS-85-5911
2 January 1985

MEMORANDUM FOR: Members and Invitees

FROM: [redacted]
Executive Secretary

STAT

SUBJECT: IG/CM Meeting

REFERENCES:
a. IG/CM memo, IG/CM Meeting, 30 November 1984 (D/ICS-84-0916)
b. Phone Conversations, 14 December 1984, IG/CM Secretariat Staff to Members/Invitees
c. IG/CM memo, Countermeasures Macro Resources Data Study Draft, 29 October 1984 (D/ICS-84-0902)
d. IG/CM memo, 7 December 1984 (D/ICS-84-0905/2)

1. Reference a. announced the date, time, and place of the fifteenth meeting of the IG/CM. Reference b. advised of the postponement of the meeting of the IG/CM until 10 January 1984. This correspondence formalizes reference b. and provides additional details.

2. The fifteenth meeting of the IG/CM will be held on Thursday, 10 January 1985, at 1400 hours. The meeting will convene in Room 6W02, [redacted] [redacted] Washington, D.C. A proposed agenda [redacted]

STAT

3. The principal purpose of the meeting is to obtain formal consensus on the Countermeasures Macro Resources Data Study in a plenary session of the IG/CM. Reference c. provided a study draft on which comments were received. A final copy of the study which assimilated those comments was provided via reference d. The goal is to transmit the IG/CM-approved study to the SIG-I as soon as possible.

4. The National Operations Security Advisory Committee (NOAC), a subcommittee of the IG/CM, has approved two items which the NOAC Chairman requests be provided to the IG/CM for information and action. Absent IG/CM objection, the NOAC intends to pursue attainment of the initial goals detailed in the OPSEC program at Attachment 2. The NOAC memorandum at Attachment 3 advises the IG/CM of NOAC approval of training objectives for a 3-tiered Community OPSEC training program and recommends that NSA be approved to act as

the lead agency responsible for developing and providing the OPSEC courses of instruction. Addressees are requested to provide concurrence or comments at the meeting. NSA will also sponsor a briefing to IG/CM attendees on the threat to super computers and recommended safeguards thereto.

5. Attendees are requested to provide names, organization, and social security number to [redacted] by COB 7 January 1985. This is required to facilitate entry into the Community Headquarters Building. STAT

[redacted] STAT

Attachments:
a/s

Attachment 1

PROPOSED AGENDA
IG/CM MEETING, 10 JANUARY 1985

I.	Opening Comments	Chairman
II.	Macro Resources Data Study	
	A. Summary	CCIS
	B. Approval	Chairman/Members
III.	NOAC Issues	
	A. National OPSEC Program Approved	Chairman/Members
	B. Training Objectives Approved	Chairman/Members
	C. NSA Lead Agency Approved	Chairman/Members
IV.	Ad Hoc Issues	Members
	Briefing: Threat to Super Computers and Safeguards Thereto	NSA

Interagency Group/Countermeasures
Washington, D.C. 20505

Attachment 2

National Operations Security Advisory Committee

National Operations Security Program

References:

a. DCI letter to National Security Advisor dated 20 May 1983 (D/ICS-83-3391)

b. IG/CM memorandum dated 6 September 1983 (D/ICS-83-0725)

c. IG/CM memorandum dated 26 January 1984

General:

Reference a. transmitted a Senior Interagency Group-Intelligence (SIG-I) approved draft National Security Decision Directive (NSDD) on Operations Security (OPSEC) and requested National Security Council (NSC) approval. The NSC has taken no promulgation action to date. Reference b. transmitted the final minutes of the 22 August meeting of the Interagency Group/Countermeasures (IG/CM) at which a National Operations Security Advisory Committee (NOAC) was established. Reference c. transmitted the approved charter for the NOAC and the agenda for the first NOAC meeting.

Overall Program Guidance:

The NOAC charter provides sufficient flexibility and authority as presently constituted. Nonetheless, a NSDD similar to that approved by the SIG-I should be promulgated so that Government agencies and departments not members of the Intelligence Community structure have authority for resource allocation.

Program Scope:

The National OPSEC Program consists of two broad areas: information aspects and operational aspects. The program outlined below will serve as the framework for the preliminary activities of the NOAC. Working groups to consider each of the areas described below may be needed to develop and formalize the details of each area.

- Informational Aspects

--National OPSEC Manual: Such a manual is needed. The working group established to prepare the manual will consider the need for definition of OPSEC and give examples of application in non-military areas. The relationship of OPSEC to security the discipline will be defined in the manual. The manual will describe the OPSEC planning and survey processes and will also describe the management of an OPSEC program. All these facets will be unclassified. In a classified supplement, Community resources available to assist in agency OPSEC programs will be cataloged. The supplement will include a generalized hostile intelligence threat statement and detail selected OPSEC lessons learned.

-- OPSEC Planning: The working group established to develop and coordinate national OPSEC training will be guided by the following considerations. Interagency training will be available at a variety of levels for OPSEC managers and planners, for OPEC support personnel, and for contractor personnel. Departments and agencies may also desire to supplement these interagency courses with agency-oriented courses. The interagency courses will be provided in such areas as OPSEC Management, OPSEC Methodology, Industrial OPSEC, and OPSEC Orientation.

- Information Sharing: NOAC members will periodically provide a summary of lessons learned in respective OPSEC programs so that such lessons can be used in interagency training courses, and in OPSEC planning and activities throughout the Government. Periodically, a compilation of these lessons learned should be appropriately distributed by the NOAC Secretariat.

- Intelligence Support: Intelligence support for OPSEC threat estimates and studies will be obtained through established channels. The NOAC will assist in prioritizing and coordinating such requests when needed. Requests for use of national assets by agencies without established channels can be made through the NOAC. Requests for finished intelligence reports can be made to the NOAC, which will forward such requests to the CCIS/ICS for scheduling.

- Operational Aspects:

  -- Prioritizing OPSEC Support: Agencies requiring OPSEC planning and survey support should (1) develop an in-house capability, (2) contract out, or (3) request assistance from other agencies. If (3) is selected, the request should be made to the NOAC, rather than to a specific agency, so that such requests can be prioritized and scheduled within the limits of available resources. Proper use of lessons learned and the use of OPSEC in planning should obviate many requests for surveys, which are expensive and time-consuming.

  -- Monitoring OPSEC Programs: The NOAC should consider primarily OPSEC issues that require multiple agency coordination or that cannot be resolved by the agencies involved. Any agency may bring an issue before the NOAC for consideration. By providing an OPSEC manual and lessons learned publications, the NOAC shall endeavor to ensure consistency in OPSEC programs as far as is appropriate.

-- OPSEC in Industry: The DoD has established a program for implementing OPSEC in contractural arrangements. Agencies participating in the Defense Industrial Security Program (DISP) have this program available to them.

-- Non-Military OPSEC: In support of the OPSEC manual, the use of OPSEC methodology in such sensitive operations as drug interdiction, funds transfers, and criminal investigations should be defined and described.

Program Priorities:

Priorities for program accomplishment will remain flexible to accommodate the exigencies of national security requirements. Nevertheless, the focus of scheduled efforts will be toward early completion of the following:

- Preparation of a National OPSEC Manual.
- Formalization of a national interagency OSPEC training program.
- Formalization of information-sharing procedures.
- Preparation of procedures for NOAC monitoring of OPSEC programs.

John F. Donnelly
Chairman, National Operations
Advisory Committee

Interagency Group/Countermeasures
Washington, D.C. 20505

Attachment 3

National Operations Security Advisory Committee

D/ICS-85-5912
2 January 1985

MEMORANDUM FOR: Chairman, Interagency Group/Countermeasures

FROM: [redacted] STAT
Executive Secretary

SUBJECT: Operations Security Training

1. At a 29 October 1984 meeting, the National Operations Security Advisory Committee (NOAC) approved a set of operations security (OPSEC) training objectives developed by a Community work group of the NOAC. It also recommended that the National Security Agency assume responsibility as the lead agency for developing and providing the national-level community courses of instruction in OPSEC. The Chairman, NOAC, has requested that these issues be referred to IG/CM for information and approval as appropriate.

2. In its deliberations, the NOAC determined that there should be three related but nevertheless distinct national-level training courses for OPSEC. One course of training will be focused on educating Executive grade personnel, another will focus on specific OPSEC training for program or project managers, and a third will provide the baseline, standard training for personnel designated as OPSEC specialists. The overall guideline objectives for these three courses of instruction are reflected in Attachments 1-3 and are provided primarily for information purposes.

3. The NOAC also recommended that the National Security Agency (NSA) be designated the lead agency for developing and providing the 3-tiered program of instruction. NSA has given preliminary indications of its willingness to accept the lead role, but cautions it can do so only with the active assistance of other agencies and departments of the Community. Through its representatives to the NOAC, members of the Intelligence Community have pledged such support. The Chairman, NOAC, requests IG/CM concurrence with the recommendation of the lead role for NSA.

[redacted] STAT

Attachments:
a/s

Attachment 1

Executive-Level OPSEC Training Objectives

1. Impart an appreciation for operations security (OPSEC) as a national concern which requires interagency planning and action; provide an understanding of the national structure and guidance for the OPSEC process.

2. Impart an appreciation of how information of intelligence value is obtained and used by an adversary to thwart US Government goals and objectives.

3. Impart a general understanding that the OPSEC process is a unique discipline in which operational considerations and intelligence and security concerns are combined under the direction of management to identify and counter specific adversary objectives against critically important, on-going and future, Government programs, operations, and functions.

4. Impart an understanding that OPSEC process objectives are to conceal or protect only that information or activity which must be exploited by an adversary to achieve his objectives.

5. Impart an understanding of what the OPSEC process means to management in terms of increased effectiveness, enhanced cost/benefits in security improvement, and personal and organizational commitment.

Attachment 2

Program/Project Manager OPSEC Training Course Objectives

1. Impart an appppreciation for OPSEC as a national concern which requires interagency planning and action; provide an understanding of the national structure and guidance for the OPSEC process.

2. Impart a general understanding of the intelligence process and how various intelligence techniques can be used to derive information.

3. Impart an appreciation of adversary capabilities, opportunities, and motivation to acquire and use information to undermine the effectiveness of political, military, economic, and technological activities of the US Government.

4. Impart an understanding that the OPSEC process is a unique discipline in which operational considerations and intelligence and security concerns are combined under the direction of management to identify and counter specific adversary objectives against critically important activities of the Government.

5. Provide a capability to define the problems and objectives of the OPSEC process and distinguish between them and those of the security disciplines.

6. Impart an understanding of OPSEC process data collection, analysis, and assessment techniques sufficient to allow the program/project manager to fulfill his role in the OPSEC process.

7. Impart an understanding of what the OPSEC process means in terms of increased effectiveness, enhanced cost/benefits in security improvement, and personal and organizational commitment.

8. Provide a capability to estimate cost, time, and resources required for OPSEC process activities, to include a basis for estimating costs of starting and maintaining an OPSEC process program and the savings ensuing from such a program.

Attachment 3

OPSEC Specialist Training Course Objectives

1. Impart a thorough understanding of how various intelligence techniques, including those of HUMINT, IMINT, and SIGINT, can be used to derive information about US Government operations, programs, and functions; enable the student to identify the potential effectiveness of those techniques against typical US Government activities; aid in identifying susceptibilities to intelligence exploitation.

2. Impart an understanding of adversary capabilities, opportunities, and motivation to acquire and use information to undermine the effectiveness of political, military, economic, and technological activities of the US Government; enable the student to identify the information needed by an adversary to degrade the effectiveness of specific US Government operations, programs, and functions; and know where to acquire intelligence information about specific adversary threats.

3. Impart an understanding that the OPSEC process is a unique discipline in which operational considerations and intelligence and security concerns are combined under the direction of management to identify and counter specific adversary objectives against critically important activities of the US Government; enable the student to distinguish between OPSEC process concerns and those of the security disciplines; and to describe the roles of management and the OPSEC specialist in the OPSEC process.

4. Impart a thorough understanding of the OPSEC process, to include:

a. a capability to collect, organize, and analyze information from a variety of sources (e.g., interviews; open source literature; directives and other prescriptive material; records and descriptive documents pertaining to logistics, communications, administration, etc.; etc.) to determine susceptibilities to intelligence collection;

b. a capability to correlate threat and susceptibility estimates to determine vulnerabilities; and

c. a capability to assess the relative significance of specific vulnerabilities.

5. Impart a capability to identify specific procedural measures and characterize technical measures needed to achieve OPSEC process objectives, enable the student to identify where assistance can be obtained for specific technical improvements.

6. Impart a capability to plan and organize OPSEC process support for on-going and future Government operations, programs, and technical support required for specific OPSEC survey and planning support activities.